

## DEVICE AND SYSTEM FOR PREVENTING COMPUTER VIRUS INVASION

Patent Number: JP5108487  
Publication date: 1993-04-30  
Inventor(s): MURAKAMI SEIJI  
Applicant(s): SEIJI MURAKAMI  
Requested Patent: ☐ JP5108487  
Application Number: JP19910292322 19911011  
Priority Number(s):  
IPC Classification: G06F12/14; G06F12/16  
EC Classification:  
Equivalents: JP8023846B

### Abstract

**PURPOSE:** To previously check invasion of computer virus and to prevent its invasion and proliferation by discriminating whether the request taken into by a request taking-in means is a correct request or the one by computer virus.

**CONSTITUTION:** A virus monitoring system A is selectively present between an application 3 and an operating system 5. The monitoring system A fetches the content of request 9 by using a request fetching means 15. Then, a requested content discriminating means 17 discriminates whether the requests 9 fetched is a correct one or the one by computer virus. When the request is the one from computer virus, an outputting means 19 rejects its request and also issues an alarm. A virus monitoring systems B and C, being present between the application and a basic BIOS 7 and a hardware 1, respectively, work similarly. These monitoring systems A-C are not the same type and selectively incorporated in.

Data supplied from the esp@cenet database - I2

特開平 5-108487

(43) 公開日 平成 5 年 (1993) 4 月 30 日

(51) Int. Cl.<sup>6</sup> 310 A 993-5 B

G 0 6 F 12/16 310 B 7629-5 B

技術表示箇所

審査請求 有 請求項の頁 2

(全 9 頁)

(21) 出願番号 特願平 3-292322

(71) 出願人 村上 清治

(22) 出願日 平成 3 年 (1991) 10 月 11 日

(72) 発明者 村上 清治

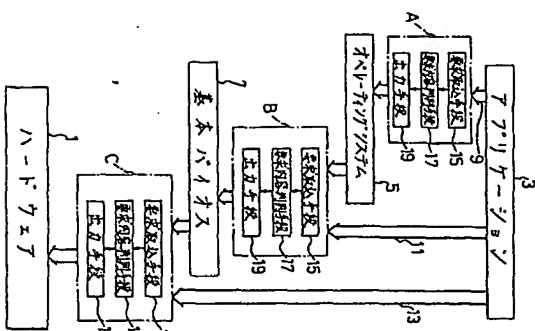
(74) 代理人 静岡県静岡市川辺町二丁目 2 番 16 号 井理士 島野 真伊智

(54) [発明の名称] コンピュータウイルス侵入防止装置と侵入防止方式

(57) [要約]

(目的) コンピュータウイルスの侵入を事前にチェックして、その侵入・増殖を防止することを可能とするコンピュータウイルス侵入防止装置と侵入防止方式を提供することを目的とする。

(構成) 例えば、アプリケーションプログラムからオペレーティングシステムへの要求を取り込み、取り込まれた要求が正常な要求か又はコンピュータウイルスによる要求かを判別し、判別結果に基づいて該要求がコンピュータウイルスによる要求の場合に少なくともその要求を禁止しようとしたものである。



[特許請求の範囲]

1  
[請求項 1] アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求、の内、少なくとも一箇所においてその要求を取り込む要求取込手段と、上記要求取込手段によって取り込まれた要求が正常な要求か又はコンピュータウイルスによる要求かを判別する要求内容判別手段と、上記要求内容判別手段の判別結果に基づいて該要求がコンピュータウイルスによる要求の場合に少なくともその要求を禁止する出力手段と、を具備したことを特徴とするコンピュータウイルス侵入防止装置。

2  
[請求項 2] アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求の内、少なくとも一箇所においてその要求を取り込み、上記取り込まれた要求が正常な要求か又はコンピュータウイルスによる要求かを判別し、上記要求内容がコンピュータウイルスによる要求の場合に少なくともその要求を禁止するようにしたことを特徴とするコンピュータウイルス侵入防止方式。

[発明の詳細な説明]

3  
[産業上の利用分野] 本発明は、コンピュータウイルス侵入防止装置と侵入防止方式に係り、特に、コンピュータウイルスが侵入して増殖する前に、これを事前にチェックしてその侵入・増殖を防止できるものに關する。

4  
[従来の技術] 昨今、コンピュータウイルスによるプログラムの破壊が大きな社会問題となつてゐる。ここに、コンピュータウイルスとは、自己増殖能力及び感染能力を持ち、ネットワーク内にはワイルドバイナリを渡し、他のコンピュータに侵入する悪性のプログラムをいう。この種のコンピュータウイルスの感染経路としては、上記したように、ネットワークを通じて侵入したり、既にコンピュータウイルスに汚染されたフロッピーディスクを使用することにより感染するものである。コンピュータウイルスに感染した場合には、画面上に不必要なメッセージが表示されたり、システムエラーが異常に増えたり、記憶されているファイルが消滅されたり、場合によってはハードディスクが破損してしまうといった症状が発生することになる。

5  
[0003] このようなコンピュータウイルスの侵入・増殖に対して、従来は次のような方法により対処していた。まず、各種ファイルに外からの書き込みを禁止する禁止禁止操作を施して、コンピュータウイルスのファイルへの侵入を防止する方法がある。又、コンピュータウイルスが感染していない正常なファイルを確認しておき、この正常なファイルと使用するファイルとを比較するこ

(2)

特開平 5-108487

6  
とにより、ファイルの感染の有無を確認するという方法がある。さらに、ファイル操作の履歴を作成し、その履歴を調べることにによりコンピュータウイルスに感染されているか否かを判別する方法もある。

7  
[0004] [発明が解決しようとする課題] 上記従来の構成によると次のような問題があった。コンピュータウイルスの侵入・増殖に対する従来の方法は、全て事後的なものである。すなわち、ファイルの任意の方法により直接操作して、コンピュータウイルスの感染の有無を確認するものであり、これでは、コンピュータウイルスの侵入・増殖を事前に防止することはできず、仮に、従来の方法によりコンピュータウイルスの感染の事実を確認できても、その時には、既に広く蔓延してしまつてゐるという可能性もあった。

8  
[0005] 本発明はこのような点に基づいてなされたものでその目的とするところは、コンピュータウイルスの侵入を事前にチェックして、その侵入・増殖を防止することを可能とするコンピュータウイルス侵入防止装置と侵入防止方式を提供することにある。

9  
[0006] [課題を解決するための手段] 上記目的を達成するべく本発明によるコンピュータウイルス侵入防止装置は、アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求、の内、少なくとも一箇所においてその要求を取り込む要求取込手段と、上記要求取込手段によって取り込まれた要求が正常な要求か又はコンピュータウイルスによる要求かを判別する要求内容判別手段と、上記要求内容判別手段の判別結果に基づいて該要求がコンピュータウイルスによる要求の場合に少なくともその要求を禁止する出力手段と、を具備したことを特徴とするものである。

10  
[0007] 又、本発明によるコンピュータウイルス侵入防止方式は、アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求の内、少なくとも一箇所においてその要求を取り込み、上記取り込まれた要求が正常な要求か又はコンピュータウイルスによる要求かを判別し、上記要求内容がコンピュータウイルスによる要求の場合に少なくともその要求を禁止するようにしたことを特徴とするものである。

11  
[0008] [作用] 本発明の場合には、アプリケーションからオペレーティングシステム又は基本バイオス又はハードウェアへの要求の内少なくとも一箇所において、その要求を取り込む、次に取り込んだ要求が正常なものであるかを判別す

る。判断した結果、コンピュータウイルスによって汚染されたものである場合には、要求を禁止するようにしたものである。

(0009) 以下、図1ないし図12を参照して本発明の一実施例を説明する。まず、図1を参照して本実施例による装置及び方式の概略を説明する。通常、各組コンピュータ及びそれを動かすソフトウェアにおいて、まず、ハードウェア1がある。このハードウェア1は、コンピュータシステムを構成する機器そのものであり、図では省略してあるが、コンピュータ本体、ディスプレイ、プリンタ、外部記憶装置、通信装置等を意味している。

(0010) 上記ハードウェア1に対してソフトウェアがあり、このソフトウェアによって上記ハードウェア1に指令を送って所望の動作を行わせるものである。上記ソフトウェアとしては、図に示すように、アプリケーション(アプリケーションプログラム)3、オペレーティングシステム5、基本バイオス7がある。上記アプリケーション3は、通常、応用プログラムと称されており、コンピュータを使用する本来の目的のためのプログラムである。又、オペレーティングシステム5は、基本プログラムの一例であり、コンピュータのハードウェア1及びソフトウェアを有効に利用するために総合管理を行うものである。さらに、上記基本バイオス7は、コンピュータの基本動作を促めたプログラム群のことであり、ハードウェア1を制御するためのものである。そして、上記ソフトウェアを制御するためのオペレーティングシステム5、基本バイオス7、ハードウェア1を適宜呼び出したり操作したりして、所望の動作を行わせることになる。

(0011) 上記アプリケーション3からオペレーティングシステム5には任意の要求9が出力される。同様に、アプリケーション3から基本バイオス7に対して任意の要求11が出力されるとともに、アプリケーション3からハードウェア1に対して任意の要求13が出力される。

(0012) 上記アプリケーション3とオペレーティングシステム5との間には、ウイルス監視システムAが選択的に介在するようになっている。このウイルス監視システムAは、要求9の内容を要求取込手段15によって取込み、取り込んだ要求9が正常なものであるかどうかを判断し、判断の結果、仮に、コンピュータウイルスによる要求である場合には、出力手段19によってアプリケーション3からオペレーティングシステム5に対する要求を禁止するとともに警告を出力するものである。又正常な場合にはオペレーティングシステム5に実行を移すことになる。尚、上記警告としては、画面上にメッセージを表示したり、或いは、ブザーを鳴らすようなことが考えられる。

(0013) 又、アプリケーション3と基本バイオス7

との間には、ウイルス監視システムBが選択的に介在するようになっている。さらに、アプリケーション3とハードウェア1との間には、ウイルス監視システムCが選択的に介在するように構成されている。これらウイルス監視システムB及びウイルス監視システムCも、上記ウイルス監視システムAの場合と同様に、要求取込手段15によって要求11又は13を取込み、取り込んだ要求11又は13を要求判断手段17によって判断し、その判断の結果、コンピュータウイルスによる要求である場合には、出力手段19によって要求を禁止するとともに警告を出力するものである。

(0014) 次に、上記ウイルス監視システムA、B、Cが、コンピュータの電源を投入してから、どのような手順でシステム内に組み込まれていくかについて、図2を参照して説明してみる。まず、電源を投入して「開始」となる。次に、ハードウェア1に合ったウイルス監視システムCが導入されるとともに、基本バイオス7の監視が行われる。次に、基本バイオス7の監視が完了したか否かの判断がなされる。基本バイオス7の監視が完了した場合には、基本バイオス7に合ったウイルス監視システムBが導入される。又、基本バイオス7の監視が完了していない場合には、再度基本バイオス7の監視を行う。

(0015) 次に、オペレーティングシステム5の監視を行う。オペレーティングシステム5の監視が完了した場合に、オペレーティングシステム5に合ったウイルス監視システムAを導入する。オペレーティングシステム5の監視が完了していない場合には、再度オペレーティングシステム5の監視を行う。そして、ウイルス監視システムAの導入が完了した時点で、システム5の組み込みが完了することになり、アプリケーション3からの要求を監視する体制ができたことになる。又、既に述べたように、ウイルス監視システムA、B、Cのそれぞれは、一種類ではなく、ハードウェア1、基本バイオス7、オペレーティングシステム5の種類のそれぞれによって任意の種類のものを選択して組み込むことになる。尚、本実施例においては、かかる一種の処理を図示しないROM上に記録するようにしている。それによって、コンピュータウイルスによる感染を防止するようにして、図10(16)次に、ウイルス監視システムA、B、Cとして、具体的にどのような方式が採られるかについて説明していく。まず、データベース法(スキャン法)から説明する。これは、各組のコンピュータウイルスによるコンピュータプログラムを予めデータベース化して記憶しておき、それが検査対象になったコンピュタプログラムに存在するか否かを判断していくものである。以下、図3を参照して説明する。まず、要求取込手段15によって要求を取り込む。次に、取り込んだ要求を解析して、判断が必要か否かを判断する。判断が必要でない場合にはそのまま処理が行われる。一方、判断が必要

な場合には、予め記憶されているデータベースのデータとの比較が行われる。そして、要求とデータベース化されたデータとが一致しない場合には、そのまま処理が行われる。又、要求とデータベース化されたデータとが一致している場合には、要求が禁止されるとともに警告・問い合わせが行われる。次に、処理が完了された場合には、プロセスが中断されることになる。

(0017) 上記データベース化されたデータとの比較・判断をさらに詳しく示すと、図4に示すようなものとなる。まず、ファイルの読み込みが行われる。次に、データベースの中から最初のデータを取り出す。そして、読み込んだファイル内容を取り出したデータと比較して一致するか否かを判断する。一致している場合には、(STC)すなわち、コンピュータウイルスに感染されているものと判断する。一方、一致していない場合には、データベースの中の全てのデータと比較したか否かが判断される。全てのデータと比較した場合には、「LC」すなわち、正常であると判断される。全てのデータと比較していない場合には、次のデータとの比較が行われる。すなわち、データベースの中から次のデータを取り出して、読み込んだファイルとの比較を行っていく。このようにして、データベースの全てのデータと比較していくことにより、コンピュータウイルスの感染の有無を判断していくものである。

(0018) 次に、バックアップ法による判断について、図5及び図6を参照して説明する。バックアップ法とは、検査対象となつていないファイルのバックアップファイルを作成・保存しておく、すなわち、ファイルの全部又は一部又はファイル内容を加工した情報をバックアップファイルとして作成・保存しておくものである。後は、検査対象のファイルと上記バックアップファイルとを比較して正常であるか否かを判断していくものである。

(0019) 以下、図を参照して詳細に説明すると、まず、図5に示すように、バックアップファイルの作成を開始する。つまり、ファイルの内容を読み込んでSUM計算、すなわち、ファイルのバイトの合計値を計算する。そして、SUMデータを出力して、そのSUM計算とファイル名とをバックアップファイル(デイスク)に記録しておく。これによって、バックアップファイルの作成が完了する。

(0020) 次に、上記で作成されているバックアップファイルを使用したバックアップ法による判断を図6を参照して説明する。まず、検査対象のファイルからデータを読み込む。次に、読み込んだデータに基づいてSUM計算を行う。次に、計算された値とバックアップファイルから取り込んだ計算値とを比較して、一致するか否かの判断がなされる。そして、一致していない場合には、「STC」すなわち、コンピュータウイルスに感

染されているものと判断される。又、一致している場合には、「LC」すなわち、正常であると判断される。

(0021) 次に、図7乃至図10を参照して接順法を採用した場合について説明する。この接順法とは、検査対象になるファイルに、ウイルスの感染の有無を判断するプログラムを予め接続しておき、システム起動時にいて、ファイル自身にウイルスの感染の有無を判断させるものである。まず、通常のファイル21は、図7に示すようになっている。本来の元プログラム23だけが記録されている。このファイル21にSUMデータ25とチェックプログラム27を接続して、接順法ファイル29を作成する。この接順法ファイル29の作成工程を示したのが図9である。すなわち、元プログラムファイルの読み込みが行われ、次に、SUM計算が行われる。次に、チェックプログラムが付加される。そして、ファイルの先頭をチェックプログラムにジャンプして、接順法ファイル29の作成が完了する。

(0022) 次に、接順法ファイル29が自身でコンピュータウイルスの感染の有無をどのような工程で判断していくかについて説明する。図10に示すように、接順法ファイル29を実行すると、チェックプログラム23のSUMを計算し、その計算値と、予め記録されているSUM値とを比較する。そして、一致している場合には正常であるとして、元プログラム23を起動する。これに対して、一致しない場合には、元プログラム23がウイルスに汚染されているとして、以後の実行を中止するものである。

(0023) 次に、キーボード法を採用した場合について説明する。このキーボード法とは、特定の動作をキーボードによって禁止する方法であり、任意のキーボードを使用しキーボードが一致した場合に以後の動作を許可するというものである。以下、図11を参照して説明する。これは、MS-DOS(登録商標)のサービスの中のファイル転送要求に対して行う場合を示すものである。まず、転送要求(AH=40)が出力される。次に、バスワート検査が行われ、バスワートが一致しない場合には、ウイルスに感染されているものと判断し、一致している場合には正常であると判断される。

(0024) 次に、手続法を採用した場合について説明する。すなわち、コンピュータウイルスに汚染されている場合に、正常な場合とは、プロセスに違いがある。これをチェックすることにより、コンピュータウイルスに感染されているか否かを判断するものである。具体的には、例えば、MS-DOS(登録商標)のサービスの要求の中にファイル転送可能サーブ要求(AH=3D02)を要求する場合、正常な場合にはファイルの属性を要求することはないが、コンピュータウイルスに汚染さ

(図1)

れている場合には、直前にファイルの属性変更 (AX=4301) を要求してくる。よって、上記ファイルの属性変更を要求するか否かによって、コンピュータウイルスに汚染されているか否かを判断することができる。上記手続法の一例を図12に示す。

(0025) 尚、ウイルス監視システムA、B、Cにおいて、上記したような方法の中からどの方法を採用して行うかについては任意であり、X、それら以外の別の方法を採用してもよい。

(0026) 以上本実施例によると次のような効果を得ることができる。まず、アプリケーション3からコンピュータウイルスによって汚染された要求が出された時点でこれをチェックし、コンピュータウイルスに汚染されているか否かを判断して、汚染されている場合には要求を中止させるとともに警告を出力するように構成している。アプリケーション3がコンピュータウイルスによって汚染されているか否かを早期に発見することができる。特に、コンピュータウイルスによる汚染の有無の確認をシステム内で自動的に行うようにしている。従来のように事後的にチェックするとは異なり、コンピュータウイルスの侵入・蔓延による被害を最小限に食い止めることができる。

(0027) X、使用するオペレーティングシステム5、基本バイオス7、ハードウェア1によって、適切なウイルス監視システムA、B、Cを自動的に選択して投入できるようにしている。使いがっつても良好である。

(0028) 尚、本発明は前記一実施例に限定されるものではない。例えば、前記一実施例では、図1に示すように、アプリケーション3、オペレーティングシステム5、基本バイオス7、ハードウェア1のそれぞれ間に、ウイルス監視システムA、B、Cを介在させるようにしたが、それらの中から任意の箇所に介在させるだけの構成も考えられる。

(0029)

(図2)

(図9)

【図面の簡単な説明】

【図1】 本発明の一実施例を示す図でコンピュータウイルス侵入防止装置の構成を示すブロック図である。

【図2】 本発明の一実施例を示す図でウイルス監視システムの投入を示すフローチャートである。

【図3】 本発明の一実施例を示す図でデータベース法による判断を示すフローチャートである。

【図4】 本発明の一実施例を示す図でデータベース法による判断を示すフローチャートである。

【図5】 本発明の一実施例を示す図でバックアップ法による判断を示すフローチャートである。

【図6】 本発明の一実施例を示す図でバックアップ法による判断を示すフローチャートである。

【図7】 本発明の一実施例を示す図で接続法による判断を示すフローチャートである。

【図8】 本発明の一実施例を示す図で接続法による判断において元のファイルを模式的に示す図である。

【図9】 本発明の一実施例を示す図で接続法による判断において接続の工程を示すフローチャートである。

【図10】 本発明の一実施例を示す図で接続法による判断を示すフローチャートである。

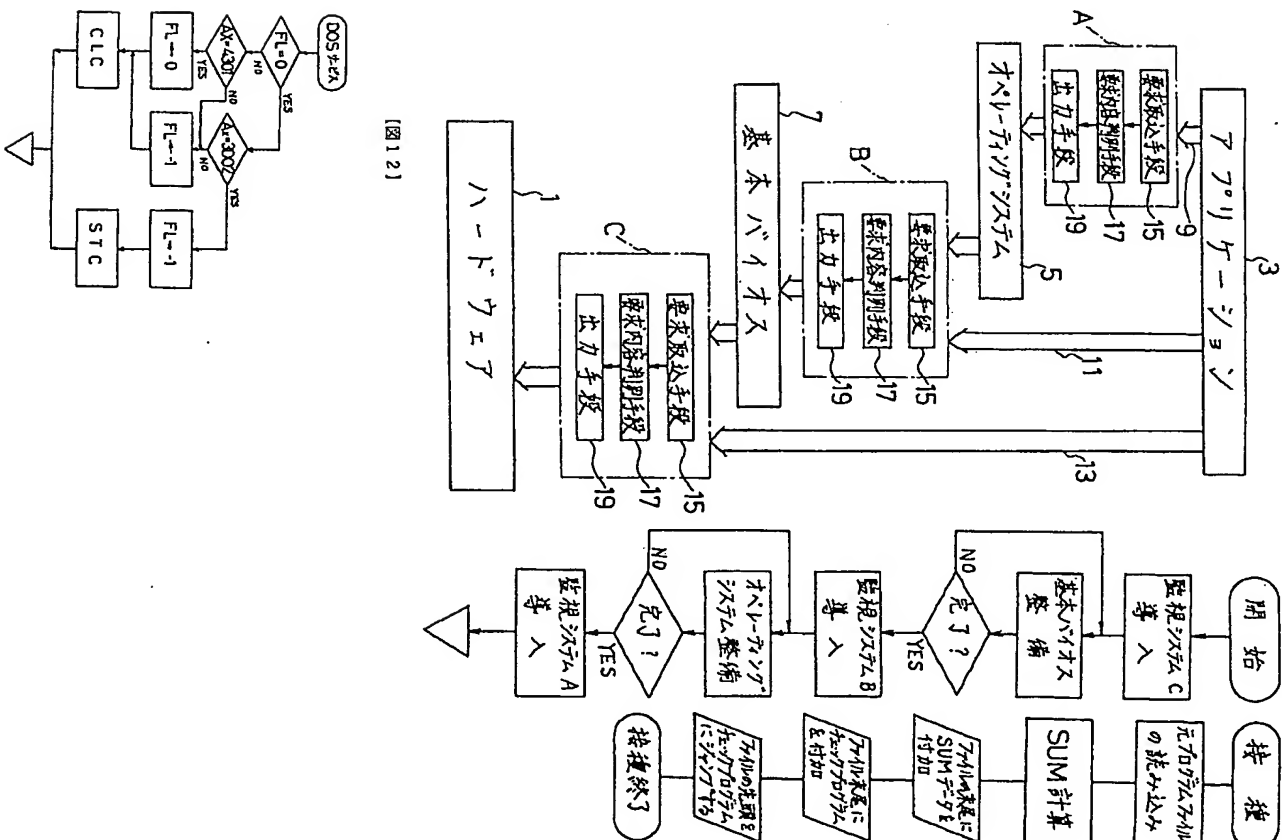
【図11】 本発明の一実施例を示す図でバスワード法による判断を示すフローチャートである。

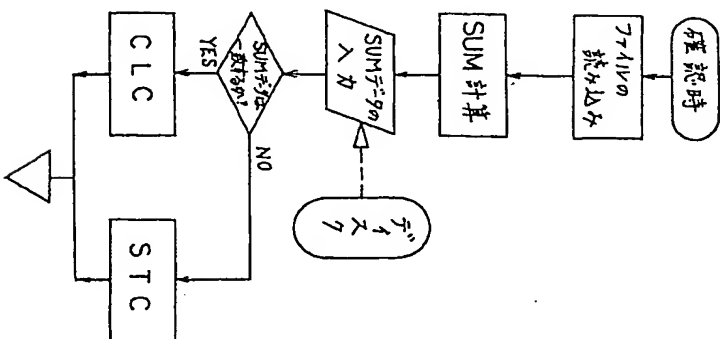
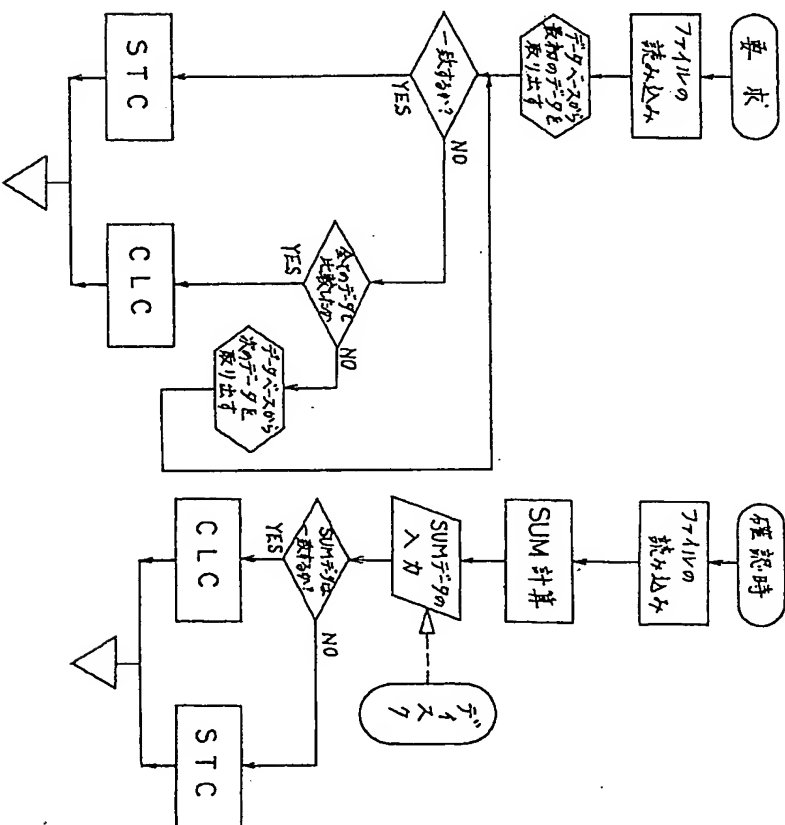
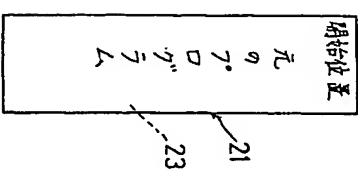
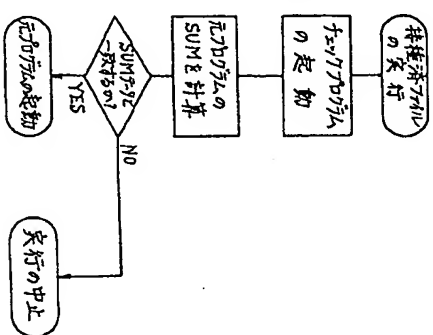
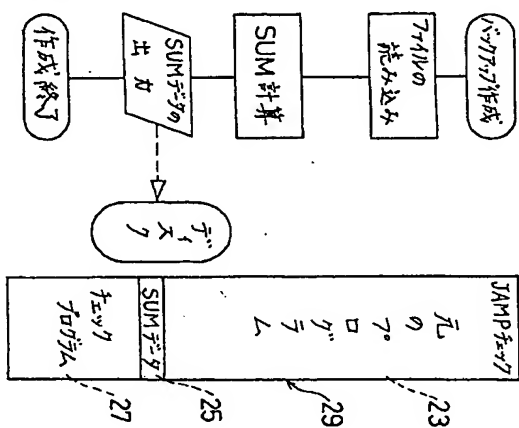
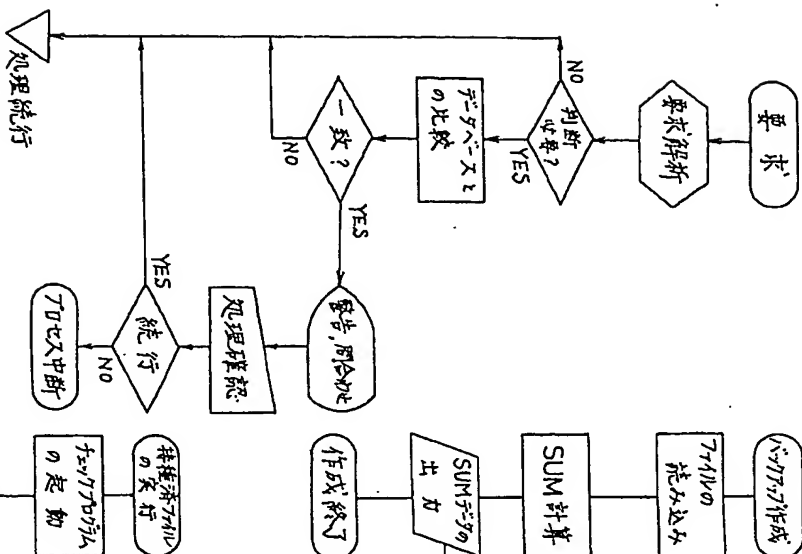
【図12】 本発明の一実施例を示す図で手続法による判断を示すフローチャートである。

【符号の説明】

1 ハードウェア  
3 アプリケーション  
5 オペレーティングシステム  
7 基本バイオス  
9 要求  
11 要求  
13 要求  
15 要求取込手段  
17 要求内容判断手段  
19 出力手段  
A ウイルス監視システム  
B ウイルス監視システム  
C ウイルス監視システム

(図12)





[図11]

